REMARKS

Claims 1-7, 9-14 and 16-36 are pending in the application with Claims 1, 9, 17, 19, 20, 22, 24, 25 and 31 being independent claims. Claims 1-7, 9-14 and 16-36 are rejected under 35 U.S.C. §103(a) as being unpatentable over Jobst (US Patent No. 6,707,915 B1). Claims 1, 17, 20 and 31 are rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. The Examiner objected to Claims 1, 9 and 17 because of informalities.

Reconsideration of the present application is respectfully requested.

Please amend Claims 1, 9 and 17 as set forth herein. No new matter has been added.

Regarding the rejection of independent Claims 1, 9, 17, 19, 20, 22, 24, 25 and 31 under 35 U.S.C. §103(a), the Examiner states that Jobst renders the claims unpatentable. With particular reference to Claims 1, 9, 25 and 31, after reviewing Jobst, it is respectfully asserted that the Examiner is incorrect. Jobst discloses a method of transferring a data packet from a providing communication terminal to a requesting communication terminal for securing a terminal against unauthorized software loading onto the phone. More particularly, a first signature is calculated using a Phone Password and a binary code of the file to be transmitted in the middle, and then the calculated first signature with the binary code of the file is transferred to a requesting phone. The requesting phone calculates a second signature based on the received binary code and previously stored Phone Password. After comparing the calculated second signature with the received first signature, the phone deems a response message to be coming from an authorized provider, if the two signatures are identical. In other words, such a comparison between the two signatures is for confirming whether it is an authorized provider for a certain selected software download because the two signatures are generated using a same signature generating algorithm. Further, the two signatures themselves are limited to be factors compared and are unique for the specific software transfer based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code. If the two signatures are not identical, the downloaded software would automatically have been deleted, not updated (in particular, see column 6, line 57-column 8, line 27). Accordingly, Jobst discloses a

confirmation of transmission in the result of the comparison of the selected software file, but does not disclose an update in case a transmitted registration identifier is different from a currently valid registration identifier in a wireless communication system, wherein broadcast data is sequentially encrypted with different encryption information, as claimed in Claims 1, 9, 25 and 31. Claims 1, 9, 25 and 31 are believed to be patentable over Jobst.

With respect to Claims 17, 19, 20, 22 and 24, it is respectfully asserted that the Examiner is incorrect. Jobst does not disclose encryption information including a predetermined mask key and lifetime information of the corresponding predetermined mask key in a wireless communication system, wherein broadcast data is sequentially encrypted with different encryption information, as claimed in Claims 17, 19, 20, 22 and 24 (see page 20, line 24-page 21, line 14; page 22, lines 11-20). Furthermore, Jobst does not disclose receiving/transmitting both current encryption information and next encryption information, as claimed in Claims 20, 22 and 24 of the present application. Jobst uses a unique identification code to verify the identity of the requesting communication terminal per a certain selected software file and to thereby check whether the data packet is provided by an authorized provider or not. Claims 17, 19, 20, 22 and 24 are also believed to be patentable over Jobst.

Regarding the rejection of independent Claims 1, 7, 20 and 31 under 35 U.S.C. §112, first paragraph, it is respectfully asserted that the Examiner is incorrect. The recitation of "the different encryption" appears to be supported in the original US application, because the present application discloses encryption information including a predetermined mask key and lifetime information of the predetermined mask key (in particular, see page 4, lines 8-10), and a plurality of different mask key transmissions for a network (in particular, see page 31, line 23-page 32, line 1 and page 33, lines 12-16).

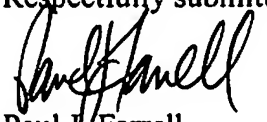
Regarding the objection to Claims 1, 9 and 17, it is respectfully submitted that the amendment to the claims set forth above as requested by the Examiner overcomes the objection.

Because the above amendments and arguments are believed to place amended independent Claims 1, 9, 17, 19, 20, 22, 24, 25 and 31 in condition for allowance, then, at least

because of their dependency on these claims respectively, dependent Claims 2-7, 10-14, 16, 18, 21, 23, 26-30 and 32-36 are also in condition for allowance.

Claims 1-7, 9-14 and 16-36 are believed to be in condition for allowance. Should the Examiner believe that a telephone conference or personal interview would facilitate resolution of any remaining matters, the Examiner may contact Applicants' attorney at the number given below.

Respectfully submitted,



Paul J. Farrell
Reg. No. 33,494
Attorney for Applicants

THE FARRELL LAW FIRM, PC
333 Earle Ovington Boulevard, Suite 701
Uniondale, New York 11553
TEL: (516) 228-3565

PJF/HY/dr